International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, August 2015
www.ijates.com
ijates
ISSN 2348 - 7550

RANDOMIZED SWAPNILs PACKET MARKING AND TRACEBACKING (RSPMT) TECHNIQUE FOR EFFICIENT IP TRACEBACK

Mr. Swapnil M. Sanap

Master of Engineering, Dept. Of Information Technology STES's S.K.N College of Engineering, Pune, Maharashtra, (India)

ABSTRACT

The an efficient packet marking technique called swapnil's packet marking and tracebacking (SPMT) technique that requires the amount of packets equal to the hop distance between the attack initiator and the server (destination) [1], which is less than 31 hops [3] [4], and can undergo certain kind of attacks like constant ID field value, and absence of router in the network chosen for marking. In this paper, we present a randomized version of SPMT called as Randomized Swapnil's packet marking and tracebacking (RSPMT) technique to avoid such attacks. Even though RSPMT may take more packets for effective traceback, it is more resilient to the kind of attacks that are possible on SPMT.

Keywords: Internet, Security, IP Protocol, IP Spoofing, IP Traceback, Denial-Of-Service (Dos) Attack, Packet Marking, Packet Tracing, Packet Filterin, Randomizer, Remainder Packet Marking.

I. INTRODUCTİON

The DoS and DDoS attacks on the networks are increasing and the result in the performance of network is decreasing. The existing packet marking and tracebacking techniques requires more number of packets to traceback the source. They also have drawbacks such as network overhead, router overhead, packet header overload, and the like. Hence in order for traceback mechanism to be competent in tracing, the mechanism should require minimum number of packets from the attacker to perform IP Traceback [1].

Thus, a mechanism which takes few or less packets and avoids all the possible overheads on packet, router, and/or network is needed for an efficient traceback of the origin of the attack. Further, the techniques must also provide a solution to mitigate the DoS and/or DDoS attacked on the network [2].

The existing tracebacking techniques take many packets for tracebacking and some of them take even thousand packets for tracebacking and hence an efficient packet marking technique called swapnil's packet marking and tracebacking (SPMT) technique as proposed in my previous paper need the packets equal to the hop distance between the attacker and the server [2], which is less than 31 [5] [6] was proposed. The proposed SPMT works on complicated DoS / DDoS attacks that may involve multiple attackers in it [2]. Further, this proposed SPMT may be utilized by other existing tracebacking techniques as well so as that the number of packets are substantially reduced for the construction of the path during tracebacking [2].

However, the proposed SPMT [2] may undergo certain kind of attacks like constant ID field value, and absence of router in the network scheduled for packet marking. In this paper, we propose a randomized version of SPMT called as Randomized swapnil's packet marking and tracebacking (RSPMT) technique to avoid such attacks. Even though RSPMT takes a little more packet for effective traceback, it is more resistive to the various attacks that may be possible on SPMT.

II. RANDOMIZED SWAPNIL'S PACKET MARKING AND TRACEBACKING (RSPMT) TECHNIQUE

Considering the basic framework as used by SPMT [2], the proposed SPMT technique uses time-to-live (TTL) value and the identification filed (ID) value of a packet to schedule the marking of the packet in the network. This algorithm may be implemented at the routers available in the network and hence, the algorithm decides which router will mark the packet. The proposed algorithm uses the TTL value to find the hop distance or the count and the ID field of the packet to value generated by the source of packet to mark the packet. In SPMT as proposed in my earlier paper the TTL value is used to find the count of the hop. A hop count of the packet and an IP ID field value of packet is used to decide if the router would mark the packet [2].

SPMT Marking Algorithm at router R [2]

Input: Packet w; Output: w: start; w: end; w: distance

1: for each packet p do
2: if ((w: ID%31) + 1) = w:hop then
3: w: start IP(router)
4: w: distance 0
5: else
6: if w: distance = 0 then
7: w: end IP(Router)
8: end if
9: increment w: distance
10: end if
11: end for

As the algorithm [2] is adapted to perform modulo arithmetic with 31, the result will always be between v Є {0, 1… 30}, and hence v + 1 Є {1… 31}. It may be understood that the value v can be equal to the hop count at only one of the routers in the path for a given IP ID value of packet.

As disclosed in the RFC 791 [7], the ID field of a packet is assigned with values generally in three ways, as shown in figure 1 below.

1) Sequential- The machine implements its own IP ID assignment counter for each session. In this all packets are marked with ID field value by the sender.

2) Sequential Jump - the communications happening using the machine has similar counter for the assignment of the ID field.

3) Random – In this technique of assignment the ID field is assigned with a value randomly. In ID values randomly generated, the ID%31 may have a result which would be uniformly distributed. It means that all the routers will have equal probability of marking the packet which would be equal to 1 to 31.

In ID values randomly generated, the ID%31 may have a result which would be uniformly distributed. It may imply that all the nodes/ routers may have equal opportunity to mark the packet which would be equal to 1/31. Hence this problem may be similar to coupon collector problem where the server/victim has to wait to get samples from each of the routers in the path to reconstruct the complete path. Expected number of packets is given by [8]:

$$E(X) = d(\ln(d) + O(1)) \text{ where } d = 31$$

Typically due to many reasons like IP header compression, the ID field of the packet is assigned with first two techniques above so that the encoding is applied efficiently. However, random packet ID field allocation/ assignment are rarely used, as the ID field is not generated randomly. The Fig. 1 below shows the assignment of packet ID field using all the three assignment techniques:

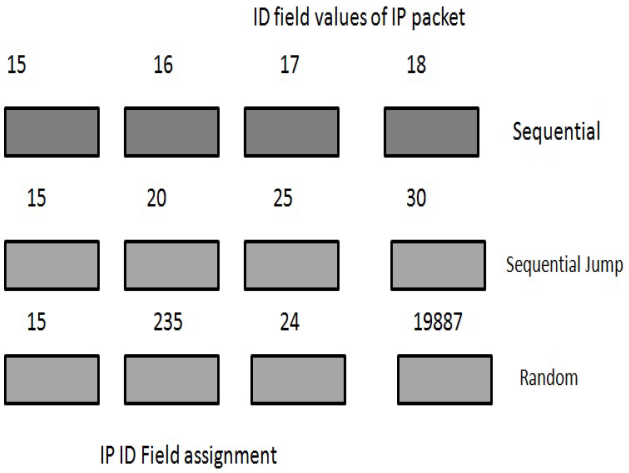

Fig. 1 IP ID field assignment

III. ATTACKS ON SPMT

Because In From the results and analysis of SPMT [2] it may be observer that the SPMT performs well and requires packets equal to number of hops by the packets for efficient traceback (even during IP spoofing attacks of source address). However, it is like that in due course of time, the attacker may realize that they can compromise SPMT if they successfully spoof / manipulate the ID field also. In the prior-art there are two ways to manipulate the ID field which are addressed as two delicate attacks as follows:

1) **Constant attack on ID:** In this type of attack, the ID field value is kept constant for a given session. Here single router is considered for marking.

2) **When the routers chosen are not present in path:** In this type of attack attacker finds out a distance in the hops to victim and assign the value of ID such that ((ID%31)+1) > d. Based on this it is possible to get hops for which routers that are also not present in the path.

To make our SPMT more robust against these and other types of attacks we present a randomized version of SPMT called randomized swapnil's packet marking and tracebacking (RSPMT) technique. This proposed RSPMT is protective against all the attacks mentioned above.

In RSPMT, the k is chosen randomly thereby avoiding reliability on only one router to mark. This randomization of the algorithm successfully prevents all the above mentioned attacks.

1) **Constant attack on ID:** When the attacker attacks the ID field using constant value, and when the "k" is selected randomly from 1 to 31, almost all the routers are eligible to mark the packet.

2) **When the routers chosen are not present in path**: Even if, the attacker may develop such ID value as the value of k will be changing thereby allowing more than one router to mark the packet.

Algorithm SPMT at router R

Input: Packet w

Output: w:start; w:end; w:distance

1: For at least one packet "p" do // The RSPMT is executed at every router on the path in the network.

2: k may be chosen randomly from "S" set = {1, 2, 3, …. 31} // For every packet passing through the router, the router generates a random number S Є {1, 2, 3, …. 31}

3: if ((w:ID%k) + 1) = w:hop then // the TTL value of packet is used to check the hop count, and it checks if ID modulo k plus one is equal to hop count.

4: w:start □ IP(router)

5: w:distance□ 0 // initializes the distance field to zero.

6: else

7: if w:distance= 0 then

8: w:end □ IP(Router)

Again 9: end if

10: increment w:distance

11: end if

12: end for

Moreover compared to PPM [1] specifically, the node sampling may still take few packets. It is also to be noted that in RSPMT a packets may be reconfigurable/ overridden. In the SPMT technique a single router is configured to mark the packet [2]. However in RSPMT, the packet can be marked by more than one routers as "k" may be chosen randomly by each router and the equation required is satisfied. Hence the last router which marks the packet wins.

IV. PATH RECONSTRUCTION FOR RSPMT TECHNIQUE

The path reconstruction procedure is common for both SPMT [2] and RSPMT. In the path reconstruction, a separate algorithm is proposed, in which the system under attack collects the malicious packets and thereby constructs a tree using the packet mark data. The complete reconstruction algorithm is given in below.

ALGORITHM:

Input: Packet w

Output: route from destination to source

1: T is a tree with root as v

2: Let the edges in the tree be (start, end, distance) tuples

3: for at least one packet "w"

4: if w.distance = 0 then

5: T.insertEdge(w.start,v,0)

7: T.insertEdge(w.start,w.end,w.distance)

8: end if

9: end for

10: any edge selected from (x, y, d) is removed with d! = distance between x to v in T

Cannot 11: extract path (Ri;…….;Rj) by enumerating acyclic paths in T (acyclic paths are extracted forming the attack paths)

V. MATHEMATICAL ANALYSIS

The problem stated above may be related to the weighted coupon collector problem. In this problem the probability of drawing different coupons c1, c2, c3… cn is p1, p2, p3… pn.

The aim is to draw coupons until we get all the coupons. In order to achieve this the proposed algorithm finds the probabilities of packets getting marked by routers some hop away from the initiator.

Let "Em" be the event, the hop distance "k" from attacker to marking router be m where m ∈ {1 … 31},

Let "Ai" be an event the router at hop "i" marks the packet. So, according to Bay's theorem:

P(Ai) = P (Ai /E1)P (E1) + P (Ai /E2)P (E2)+ P (Ai /E3)P (E3) + …… + P (Ai /E31)

Where,

Ak with equal probability is chosen randomly hence

P(Em)=1/31m ε m ∈ {1 … 31}

$$P(A1) = 1.\frac{1}{31} + \frac{1}{2}.\frac{1}{31} \dots + \frac{1}{31}.\frac{1}{31} = \frac{1}{31}(\frac{1}{1} + \frac{1}{2} \dots \dots + \frac{1}{31})$$

$$P(A2) = 0.\frac{1}{31} + \frac{1}{2}.\frac{1}{31} \dots + \frac{1}{31}.\frac{1}{31} = \frac{1}{31}(\frac{0}{1} + \frac{1}{2} \dots \dots + \frac{1}{31})$$

$$P(A3) = \frac{0}{2}.\frac{1}{31} + \frac{0}{2}.\frac{1}{31} + \frac{1}{3}.\frac{1}{31} \dots + \frac{1}{31}.\frac{1}{31} = \frac{1}{31}(\frac{0}{1} + \frac{0}{2} + \frac{1}{3} \dots \dots + \frac{1}{31})$$

$$P(A4) = \frac{0}{2}.\frac{1}{31} + \frac{0}{2}.\frac{1}{31} + \frac{0}{3}.\frac{1}{31} + \frac{1}{4}.\frac{1}{31} \dots + \frac{1}{31}.\frac{1}{31} = \frac{1}{31}(\frac{0}{1} + \frac{0}{2} + \frac{0}{3} + \frac{1}{4} \dots \dots + \frac{1}{31})$$

Hence the probability P (EPMr) that the finally router at hop r marks the packet and the mark is not overwritten will be possible only if router at hop r marks the packet and then no other router marks the packet. The probability is given by the following equation

P(EPMr)=P(Ar)·(1 − P (Ar+1))·(1 − P (Ar+2))……(1 – P (A31))

$$= \frac{1}{31}.\sum_{n=r}^{31}\frac{1}{n}.\left(1 - \frac{1}{31}.\sum_{n=r+1}^{31}\frac{1}{n}\right).\left(1 - \frac{1}{31}.\sum_{n=r+2}^{31}\frac{1}{n}\right) \dots \dots \left(1 - \frac{1}{31}.\frac{1}{31}\right)$$

If number of hops is less than 31 let us say H, then the equation is-

P(EPMr)=P(Ar)·(1 − P (Ar+1))·(1 − P (Ar+2))……(1 – P (AH)) is decreasing function of r.

We Prove next that the probabilities P(EPM1) < P(EPM2) < P(EPM3) < ……. < P(EPMn) i.e., P(EPMr) is decreasing function of r.

Proof:

P(EPMr)=P(Ar)•(1 − P (Ar+1))•(1 − P (Ar+2))……(1 – P (AH))

P(EPMr+1)=(1 − P (Ar+1))•(1 − P (Ar+2))……(1 – P (AH))

(P(EPMr))/(P(EPMr+1))=(P(Ar))/(P(EPMr+1)) .(1 - P (Ar+1)

=(1/31.∑_(n=r)^31▒1/n)/(1/31.∑_(n=r+1)^31▒1/n) .(1- 1/31.∑_(n=r+1)^31▒1/n)

=(∑_(n=r)^31▒1/n- ∑_(n=r+1)^31▒1/31)/(∑_(n=r+1)^31▒1/n)

=(1/r+ 30/31 ∑_(n=r+1)^31▒1/n)/(∑_(n=r+1)^31▒1/n)

=1/(r∑_(n=r+1)^31▒1/n)+ 30/31

=f+ 30/31 where f> 1/2

> 1

Hence the probability function is monotonically decreasing. There is also a small chance of the packet remaining unmarked. This is possible if none of the routers generate k such that packet can be marked by it. The probability that the packet remains unmarked is given by

P(EPMum) = (1 − P (A1)·(1 − P (A2)……(1 – P (AH))

We observed that lesser the number of hops greater is the probability of packet being marked.

Now we will use the weighted Coupon Collector problem or Coupon Collector with unequal probability to calculate number of packets required for path reconstruction. Let p1; p2; p3; ……; pn be probabilities of getting packets marked by router at hop 1; 2; 3; …. n. Then expected number of packets required is given by [9]

$$E(X) = \sum_{1<i1<n} \frac{1}{pi1} - \sum_{1<i1<i2<n} \frac{1}{pi1+pi2} + \ldots\ldots + (-1)^{n-1} \frac{1}{p1+p2+p3\ldots+pn}$$

This is exact equation for finding expected number of packets before I can perform successful path reconstruction. However it requires exponentially large number of calculations as the number of coupons increases. I use an approximation for this equation given above. In weighted coupon collector case where in each step every coupon i is drawn with probability pi. Let p= (p1, p2, p3… pn).

In this setting exact but complicated bounds are known for E[C(p)], which is the expected time to obtain all n coupons. Here I use the following rather simple way to approximate E[C(p)], as given in [9]

Assume p1 < p2 < …. < pn then as an approximation. This expression approximates E[C(p)] by a factor of θ(log log n).

VI. RESULTS OF SIMULATION

In this section, we try to analyze how RSMPT performs in comparison with the PPM packet marking technique. We simulate our algorithm in NS-2 simulator having Network animator as front end and TCL as back end scripting language. We have written small code to simulate PPM, and SMPT. The Parameters analyzed / calculated for the successful implementation of the proposed RSPMT. In Fig. 2 we try to compare number of packets required in case of RSPMT and PPM with different probabilities p. We see that RSPMT performs much better than PPM for different probability values.

In Fig. 3 the packets required for path reconstruction for RRSPMT in case of sequential ID values and random ID values and other existing techniques are compared. It is clearly seen that that RSPMT performs equally well in case of both sequential and random ID values.

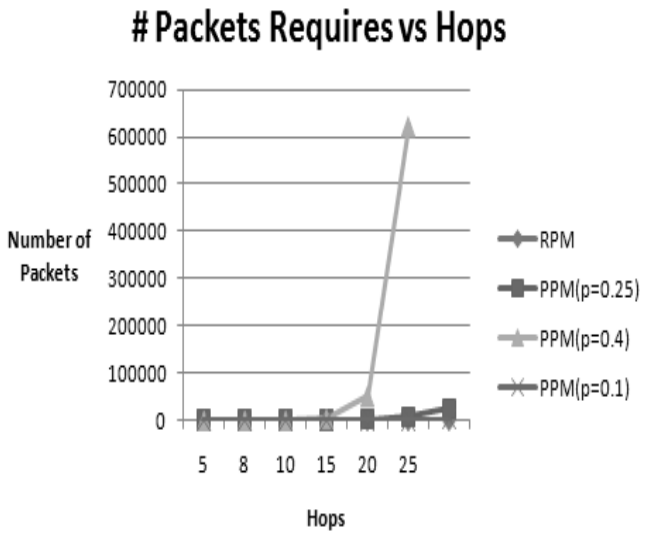

Fig. 2 Marking probability by routers vs distance in hops for RSPMT

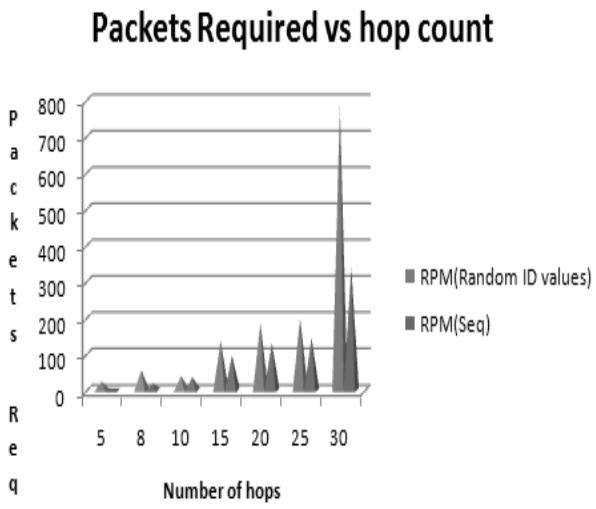

Fig. 3 Marking probability by routers vs distance in hops for RSPMT

V. CONCLUSION

The SMPT mechanism [2] that takes few or less packets and avoids all the possible overheads on packet, router, and/or network is proposed for an efficient traceback of the origin of the attack, however, the SPMT may undergo certain kind of attacks like constant ID field value, and absence of router in the network chosen for marking. In this paper, a randomized version of SPMT called as Randomized Swapnil's packet marking and tracebacking (RSPMT) technique is proposed to avoid such attacks. Even though RSPMT takes a little more packet for efficient traceback, it is more robust to the kind of attacks that are possible on SPMT. Further, the techniques also provide a solution to mitigate the DoS and/or DDoS attacked on the network.

REFERENCES

[1] Swapnil M. Sanap, and Pranav Pawar; March 2015 "overview of ip tracebacking using packet marking techniques", ICACEA, 2015, IEEE transaction.

[2] Swapnil M. Sanap; November 2015 "Swapnils packet marking and tracebacking (SPMT) technique for efficient IP traceback", IEEE International Conference on Communication, Control & Intelligent System (CCIS 2015).

[3] Savage, Stefan; D. Wetherall, A. Karlin, and T. Anderson (2000), "ACM SIGCOMM", Stockholm, Sweden. Retrieved 2008-11-18

[4] Shui Yu; 2014 "Attack Source Traceback", Springer Briefs in Computer Science, PP 55-75.

[5] C.Partridge A.C.Snoeren and C.E.Jones, "Hash-based IP Traceback", ACM SIGCOMM, 2001.

[6] A. Perrig A.Yaar and D. Song, "StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks", Technical Report, CMU, 2003.

[7] J. Postel, "Internet protocol", RFC 791, Internet Engineering Task Force, Sept. 1981.

[8] A. Karlin. S.Savage. "Practical Network Support for IP Traceback:, ACM SIGCOMM, pages 295-306, 2000.

[9] Berenbrink, Petra and Sauerwald Thomas, 'The Weighted Coupon Collector Problem and Applications' Springer, COMPUTING AND COMBINATORICS Lecture Notes in Computer Science, 2009.